Your Mobile Device and Health Information Privacy and Security

http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

1. Use a password or other user authentication

Authentication is the process of verifying the identity of a user, process, or device. Mobile devices can be configured to require passwords, personal identification numbers (PINs), or passcodes to gain access to it. The password, PIN, or passcode field can be masked to prevent people from seeing it. Mobile devices can also activate their screen locking after a set period of device inactivity to prevent an unauthorized user from accessing it.

Read More

2. Install and enable encryption

Encryption protects health information stored on and sent by mobile devices. Mobile devices can have built-in encryption capabilities, or you can buy and install an encryption tool on your device.

Read More

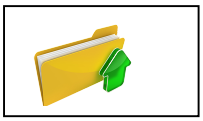
3. Install and activate remote wiping and/or remote disabling

Remote wiping enables you to erase data on a mobile device remotely. If you enable the remote wipe feature, you can permanently delete data stored on a lost or stolen mobile device.

Remote disabling enables you to lock or completely erase data stored on a mobile device if it is lost or stolen. If the mobile device is recovered, you can unlock it.

Read More

4. Disable and do not install or use file sharing applications



File sharing is software or a system that allows Internet users to connect to each other and trade computer files. But file sharing can also enable unauthorized users to access your laptop without your knowledge. By disabling or not using file sharing applications, you reduce a known risk to data on your mobile device.

Read More

5. Install and enable a firewall

A personal firewall on a mobile device can protect against unauthorized connections. Firewalls intercept incoming and outgoing connection attempts and block or permit them based on a set of rules.

Read More

6. Install and enable security software

Security software can be installed to protect against malicious applications, viruses, spyware, and malware-based attacks.

Read More

7. Keep your security software up to date

When you regularly update your security software, you have the latest tools to prevent unauthorized access to health information on or through your mobile device.

Read More

8. Research mobile applications (apps) before downloading

A mobile app is a software program that performs one or more specific functions. Before you download and install an app on your mobile device, verify that the app will perform only functions you approve of. Use known websites or other trusted sources that you know will give reputable reviews of the app.

Read More

9. Maintain physical control

The benefits of mobile devices - portability, small size, and convenience - are also their challenges for protecting and securing health information. Mobile devices are easily lost or stolen. There is also a risk of unauthorized use and disclosure of patient health information. You can limit an unauthorized users' access, tampering or theft of your mobile device when you physically secure the device.

Read More

10. Use adequate security to send or receive health information over public Wi-Fi networks

Public Wi-Fi networks can be an easy way for unauthorized users to intercept information. You can protect and secure health information by not sending or receiving it when connected to a public Wi-Fi network, unless you use secure, encrypted connections.

Read More

11. Delete all stored health information before discarding or reusing the mobile device

When you use software tools that thoroughly delete (or wipe) data stored on a mobile device before discarding or reusing the device, you can protect and secure health information from unauthorized access. HHS OCR has issued guidance that discusses the proper steps to take to remove health information and other sensitive data stored on your mobile device before you dispose or reuse the device.

Read More